REMARKS

The present application and its claims are directed to a mobile application security system. Claims 1-20 were originally presented and Claim 21 has been added so that Claims 1- 21 are presented for consideration by the Examiner.

OBJECTION TO SPECIFICATION

Applicant has amended the "Related Applications" paragraph to list the missing application number so that this objection has been overcome and should be withdrawn. Applicant requests the Examiner to acknowledge Applicant's domestic priority claims.

INFORMATION DISCLOSURE STATEMENT

Applicant understands that the Examiner has objected to the IDS filed on November 21, 2001 as some of the references did not list a publication date. In response, Applicant is submitting herewith another IDS with those references wherein the publication dates of those references are listed on the 1449 form.

JUMPING BEANS WHITE PAPER

Applicant has noted the Examiner's questions about the Jumping Beans White Paper dated December, 1998 (the "White Paper") referred to in Jansen. Applicant is submitting this White Paper in an Information Disclosure Statement accompanying this response so that the White Paper may be considered by the Examiner and placed into the file. Briefly, the White Paper is a general description of a mobile application system. The invention claimed in this application evolved from the mobile application system described in the White Paper, but the White Paper does not describe the details of a mobile application security system set forth in the claims of this application.

PRIOR ART REJECTIONS

In response to the Examiner's rejection of Claims 1-20 under 35 U.S.C. 102(a) as being anticipated by Jansen et al., NIST Special Publication 800-19- Mobile Application Security (hereinafter "Jansen"), Applicant respectfully traverses the rejection. In particular, the claims are not anticipated by Jansen, for the reasons set forth below, and early allowance of the claims is respectfully requested.

Claims 1, 6 and 11

Claim 1 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central security enforcement node further comprising means for monitoring the security of the mobile application as it jumps between the nodes wherein data about the mobile application is communicated to the central security enforcement node when the mobile application is communicated from a first node to a second node" as set forth in the claim. To support his rejection, the Examiner cites to pages 13-14 and 18-19. At pages 13-14, Jansen teaches a "reference monitor" that establishes separate isolated domains for each agent and the platform and controls all inter-domain access. At pages 18-19, Jansen, citing to the Jumping Beans system, describes a system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central security enforcement node. The Jumping Beans systems as described in the Jansen article, has a secure central host, but Jansen does not describe that the Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central security enforcement node when the mobile application is communicated from a first node to a second node. Furthermore, the description of the reference monitor does not describe that the reference monitor is a central security enforcement node as set forth in the claim and does not teach the elements set forth in the claim. Thus, Jansen does not teach this element.

In addition, Claim 1 is not anticipated by Jansen for the reason that Jansen does not disclose "the security monitoring means further comprises means for detecting unwanted changes in the code associated with the mobile application when the mobile application is jumping between hosts." The Examiner has cited Sections 2.2.4 and 2.3.4 of Jansen to support

his rejection of this element of Claim 1. Section 2.2.4 teaches that the modification of an agent's code is a particularly insidious form of attack. Jansen also describes using signed code to solve this problem. However, the signed code described in Jansen does not permit a trusted host to modify the code of a mobile application (as it might do), requires each host to maintain a list of the trusted hosts and requires the secure distribution of the public keys. This signed code is not a central security enforcement node that monitors the security of the mobile application.

Section 2.3.4 of Jansen teaches that a platform must be prevented from modifying an agent's code, state or data without being detected and describes some examples of this problem. Jansen also describes that an original author can sign the agent's code to prevent changes in the code. Jansen then describes that a multi-hop scenario is more risky than a single hop problem. Thus, in Section 2.3.4, Jansen teaches 1) that code modification is bad; 2) that a digital signature may prevent some code modification; and 3) that multi-hop risks are higher since the mobile application is farther away from its home platform. Thus, Jansen describes the problem, but one again does not offer any solution to the problem. Furthermore, nothing in Jansen teaches or suggests that a central security enforcement node detects unwanted changes in the code associated with the mobile application when the mobile application is jumping between hosts as set forth in the claim. Thus, Jansen does not disclose or suggest the invention recited in Claim 1. Claims 6 and 11 are allowable over Jansen for at least the same reasons as Claim 1.

Claims 2 and 12

Claim 2 is allowable for at least the same reasons as Claim 1 above. In addition, Claim 2 is not anticipated by Jansen as Jansen does not teach that a central security enforcement node stores a copy of a mobile application and then compares it to the mobile application from another node as set forth in the claim. To support the rejection, the Examiner cited in Section 3.2 of

Jansen and states "1st paragraph teaches protecting against modification of code, ie. comparing the original to the one received." However, the second portion of the statement by the Examiner does not logically follow from the first part as there are many different ways to protect against code modification and the first statement does not in any way imply or suggest the conclusion made by the Examiner. Therefore, there is no support in Section 3.2 for the Examiner's rejection.

Furthermore, the Examiner has relied on Section 4.2.2 of Jansen that discusses mutual itinerary recording to support his rejection. However, Section 4.2.2 describes that the itinerary of the mobile agent is recorded by another agent and used to detect malicious platform behavior. However, this section of Jansen does not describe that the copy of the mobile agent (which is different from the itinerary) is made and then the stored copy may be compared to a mobile application from another node. Jansen's system attempts to catch inconsistencies in the itineraries of the mobile agents, but would not detect other code modifications of the mobile agent. In addition, the system in Jansen does not describe that the elements set forth in this claim are at the central security enforcement node as claimed.

Finally, the Examiner cites to the lists/tables at the bottom of page 14 and at the top of page 19 in Jansen to support his rejection of this claim. However, none of the items listed on page 14 or page 19 disclose (or even suggest) that a central security enforcement node stores a copy of a mobile application and then compares it to the mobile application from another node as set forth in the claim. It is hard to imagine how one of ordinary skill in the art would use the claimed mobile application comparison element when it is not even suggested in the Jansen article. Thus, the lists do not support the Examiner rejection of this claim and Claim 2 is allowable over Jansen.

Similarly, Claim 12 is allowable over Jansen for at least the same reasons as Claim 1 and is further allowable over Jansen for at least the same reasons as Claim 2 above.

Claim 3

Claim 3 is not anticipated by Jansen for at least the same reason as Claim 1.

Claims 4 and 13

Claim 4 is allowable over Jansen for at least the same reasons as Claim 1. In addition, Jansen does not teach "wherein the security monitoring means further comprises means for preventing a node from transmitting hostile code in a mobile application to another node." The Examiner has cited to IBM Aglets discussion on page 19 of Jansen to support his rejection of this element of the claim. However, it is clear from the description that the Aglets system does not have a central security enforcement node and that the Aglets system does not have a central security enforcement node that prevents a node from transmitting hostile code in a mobile application to another node. Furthermore, in the Aglets system, each host must block the mobile application which is different from a central security enforcement node performing that task. In addition, the Aglets system does not prevent a node from transmitting the hostile code as claimed, but only blocks the mobile application at a particular host. Therefore, Claim 4 is allowable over Jansen. Claim 13 is allowable over Jansen for at least the same reasons as Claim 4.

Claims 5 and 14

Claim 5 is allowable over Jansen for at least the same reasons as Claim 4. In addition, Jansen does not disclose "means for stripping the code from an initially received mobile application if the host is not trusted, means for saving the code of the mobile application, and means, when requested by another node, for providing the code for the mobile application to the

requesting node" as set forth in the claim. The Examiner states that "many options exist as to how to stay safe from said machine [the untrusted host]..." on page 5 of the Office action, but never cites to a portion of Jansen that discloses the elements set forth in Claim 5. In fact, Jansen does not disclose the elements recited in Claim 5 and therefore Claim 5 is allowable over Jansen.

Claim 7

Claim 7 is allowable for at least the same reasons as Claim 6 from which it depends and as Claim 2 above.

Claims 8- 10

Claim 8 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central security enforcement node further comprising means for monitoring the security of the mobile application as it jumps between the nodes wherein data about the mobile application is communicated to the central security enforcement node when the mobile application is communicated from a first node to a second node" as set forth in the claim. To support his rejection, the Examiner cites to pages 13-14 and 18-19. At pages 13-14, Jansen teaches a "reference monitor" that establishes separate isolated domains for each agent and the platform and controls all inter-domain access. At pages 18-19, Jansen, citing to the Jumping Beans system, describes a system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central security enforcement node. The Jumping Beans systems as described in the Jansen article, has a secure central host, but Jansen does not describe that the Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central security enforcement node when the mobile application is communicated from a first node to a second node. Furthermore, the

description of the reference monitor does not teach a claimed central security enforcement node and does not teach the elements set forth in the claim. Thus, Jansen does not teach this element.

In addition, Claim 8 is not anticipated by Jansen for the reason that Jansen does not disclose "the security monitoring means further comprises means for detecting unwanted changes in the itinerary associated with the mobile application when the mobile application is jumping between hosts." The Examiner has cited Sections 2.2.4 and 2.3.4 of Jansen to support his rejection of this element of Claim 1. Section 2.2.4 teaches that the modification of an agent's code is a particularly insidious form of attack. Jansen also describes using signed code to solve this problem. However, the signed code described in Jansen does not permit a trusted host to modify the code of a mobile application (as it might do), requires each host to maintain a list of the trusted hosts and requires the secure distribution of the public keys. This signed code is not a central security enforcement node that monitors the security of the mobile application.

Section 2.3.4 of Jansen teaches that a platform must be prevented from modifying an agent's code, state or data without being detected and describes some examples of this problem. Jansen also describes that an original author can sign the agent's code to prevent changes in the code. Jansen then describes that a multi-hop scenario is more risky than a single hop problem. Thus, in Section 2.3.4, Jansen teaches 1) that code modification is bad; 2) that a digital signature may prevent some code modification; and 3) that multi-hop risks are higher since the mobile application is farther away from its home platform. Thus, Jansen describes the problem, but once again does not offer any real solution to the problem. Although Jansen does discuss that the itinerary of a mobile agent may be stored, Jansen does not disclose that the itinerary of the mobile agent is stored at a central security enforcement node or that the central security enforcement node detected unwanted changes in the itinerary of the mobile application. Thus,

Jansen does not disclose or suggest the invention recited in Claim 8. Claims 9 and 10 are allowable over Jansen for at least the same reasons as Claim 8.

Claims 15 - 16

Claim 15 is allowable over Jansen for at least the same reasons as Claim 1. Claim 16 is allowable for at the same reasons as Claim 15 from which it depends and Claim 2 above.

Claims 17-19

Claims 17-19 are allowable over Jansen for at least the same reasons as Claims 8-10 above.

Claim 20

Claim 20 is not anticipated by Jansen for at least the same reasons as Claim 1 above. Furthermore, Jansen does not disclose "wherein the security monitoring further comprises preventing untrusted hosts from initially launching mobile applications" as set forth in the claim. The Examiner points out that "a non-trusting host launching a mobile application reads on hostile code" in his rejection. Even assuming that the above statement is correct (which it is not), it is unclear how Jansen therefore discloses that the central security enforcement node prevents untrusted hosts from initially launching mobile applications. At most, Jansen describes the Aglet system that blocks an incoming mobile application which is very different from preventing untrusted hosts from initially launching mobile applications as set forth above. Thus, Jansen does not disclose this feature and therefore Claim 20 is allowable over Jansen.

Claim 21 is allowable over Jansen for at least the same reasons as Claim 20.

CONCLUSION

In view of the above, it is respectfully submitted that Claims 1-21 are allowable over the prior art cited by the Examiner and early allowance of these claims and the application is respectfully requested.

The Examiner is invited to call Applicant's attorney at the number below in order to speed the prosecution of this application.

The Commissioner is authorized to charge any deficiencies in fees and credit any overpayment of fees to Deposit Account No. 07-1896.

Respectfully submitted,

GRAY CARY WARE & FREIDENRICH LLP

Dated: March 18, 2004 By _____

Timothy W. Lohse
Reg. No. 35,255
Attorney for Applicant

GRAY CARY WARE & FREIDENRICH
2000 University Avenue
East Palo Alto, CA 94303
Telephone: (650) 833-2055

Gray Cary\EM\7161721.1
1010722-991103

Gray Cary\EM\7161721.1
1010722-991103